

תזכורת: תהי G חבורה ו $g \in G$, $o(g) = \min\{n \in \mathbb{N} : g^n = e\}$. אם הקבוצה הנ"ל ריקה, אומרים שהסדר של g הוא אינסוף.

בהרצאה הוכחתם: $g^m = e$ אם $m | o(g)$.

תרגיל: הוכיחו ש $o(g) = o(g^{-1})$.

הוכחה: נוכיח שוויון של הקבוצות הבאות:

$$\{n \in \mathbb{N} : g^n = e\} = \{n \in \mathbb{N} : (g^{-1})^n = e\}$$

נוכיח הכלה דו כיוונית.

למעשה, מספיק להראות כיוון אחד, כי הכיוון השני הוא סימטרי, כי אפשר לסמן $h = g^{-1}$,

ואז $g = h^{-1}$.

$\{n \in \mathbb{N} : g^n = e\} \subseteq \{n \in \mathbb{N} : (g^{-1})^n = e\}$ נניח ש $g^n = e$.

אם האיברים שווים, ההופכי שלהם שווה (אמ"ם).

$$(g^n)^{-1} = e^{-1}$$

$$(g^{-1})^n = e$$

קיבלנו שהקבוצות שוות. ולכן אם אחת ריקה גם השנייה ריקה (כלומר, הסדר של g הוא אינסוף אמ"ם הסדר של g^{-1} הוא אינסוף), ואם הן לא ריקות יש להן את אותו מינימום.

תרגיל: תהי G חבורה. הוכיחו/הפריכו:

$$H = \{g \in G : \exists n \in \mathbb{N} : g^n = e\}$$

היא תת חבורה.

פתרון:

הפרכה: נקח $G = GL_n(\mathbb{F})$

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

$$a^2 = -I, a^4 = I$$

ולכן $o(a) = 4$

$$b^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, b^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$o(b) = 3$

$$ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq I$$

לכל n טבעי.

תרגיל המשך: תהי G חבורה אבלית. הוכיחו ש

$$H = \{g \in G : \exists n \in \mathbb{N} : g^n = e\}$$

היא תת חבורה.

פתרון: הוכחה:

1. $e \in H$. ברור כי $e^1 = e$.

2. סגירות להופכי: נניח $g \in H$, זה אומר שהסדר שלו סופי. הוכחנו ש $o(g) = o(g^{-1})$ ולכן גם $g^{-1} \in H$, כלומר, $g^{-1} \in H$.

3. סגירות לכפל: נניח $g, h \in H$. נניח ש $o(g) = n, o(h) = m$.

$$(gh)^{nm} = g^{nm} h^{nm} = (g^n)^m (h^m)^n = e^m e^n = e$$

לכן $gh \in H$

הגדרה: G נקראת ציקלית אם קיים $g \in G$ כך ש $\langle g \rangle = G$.

דוגמאות: $\mathbb{Z} = \langle 1 \rangle$

$\mathbb{Z}_n = \langle 1 \rangle$

הערה: ראיתם בהרצאה שאם $G = \langle g \rangle$, אז $|G| = o(g)$.

למעשה, אם G חבורה סופית, אז G ציקלית אם"ם קיים איבר מסדר $|G|$

דוגמא: האם U_{12} היא ציקלית?

פתרון: U_{12} זה אוסף האיברים שזרים ל 12, עם פעולת כפל מודולו 12.

$$U_{12} = \{1, 5, 7, 11\}$$

5, 1

7, 1

11, 1

כל האיברים מסדר 2 ולכן החבורה לא ציקלית.

האם $\mathbb{Z}_3 \times \mathbb{Z}_4$ ציקלית?

פתרון: בחבורה יש 12 איברים. האם יש איבר מסדר 12?

בסוף התרגול הקודם, הוכנו שהסדר של (g, h) הוא $\text{lcm}(o(g), o(h))$.

$\mathbb{Z}_3, \mathbb{Z}_4$ הן ציקליות, ולכן יש בהן איבר מסדר 3 ואיבר מסדר 4, בהתאמה. אז הזוג הסדור של

האיברים האלה הוא מסדר 12.

$$(1, 1), (2, 2), (0, 3), (1, 0), (2, 1) \dots$$

שאלה: יהי $n \geq 2$. האם $\mathbb{Z}_n \times \mathbb{Z}_n$ ציקלית?

פתרון: בחבורה יש n^2 איברים. לכל $a \in \mathbb{Z}_n$, $o(a) \leq n$.

$$o(a, b) = \text{lcm}(o(a), o(b)) \leq o(a)o(b) \leq n^2$$

המכפלה יכולה לצאת n^2 רק כאשר שניהם שווים ל- n . אבל אז ידוע שהמכפלה המשותפת המינימלית היא n .

לכן לא קיים איבר מסדר n^2 .

$$o(a^d) = \frac{n}{(d, n)} \text{ או } o(a) = n, \text{ אם } o(a) = n$$

מסקנה: אם G ציקלית סופית אז יש לה יוצר, איבר g מסדר $|G|$. כמה יוצרים יש ל- G ?
 פתרון: כל האיברים ב- G הם מהצורה g^d כאשר $d \in \mathbb{N}$. הסבר: אין צורך להשתמש בחזקות שליליות, כי יש סדר סופי, נניח $g^n = e$, או $g^{-1} = g^{n-1}$. מספר היוצרים שווה למספר האיברים שהסדר שלהם הוא n . $o(g^d) = \frac{n}{(d, n)}$. לכן $o(g^d) = n$ רק כאשר $(d, n) = 1$. לכן מספר היוצרים שווה למספר המספרים שזרים ל- n , כלומר $\varphi(n)$.
 בחזרה ל- $\mathbb{Z}_3 \times \mathbb{Z}_4$. יש לה 4 יוצרים. ראינו ש- $(1, 1)$ יוצר. אבל הוא לא היחיד.

$$(1, 1)^1, (1, 1)^5, (1, 1)^7, (1, 1)^{11}$$

$$(1, 1), (2, 1), (1, 3), (2, 3)$$

משפט לגראנז': תהי G חבורה סופית, לכל $g \in G$, $o(g) \mid |G|$.

תרגיל: תהי G חבורה לא אבלית מסדר 8. הוכיחו שיש ב- G איבר מסדר 4.
 פתרון: הסדרים האפשריים בחבורה הם 1, 2, 4, 8. יש רק איבר אחד מסדר 1, איבר היחידה. אם היה איבר מסדר 8 החבורה הייתה ציקלית ולכן אבלית. סתירה לנתון. לכן אין איבר מסדר 8. בתרגול הראשון הוכחנו שאם כל באיברים מסדר 2 (כלומר, מקימים $g^2 = e$) זה אומר שחוץ מהיחידה כולם מסדר 2. אז החבורה אבלית. לכן יש איבר מסדר 4. מש"ל.

שאלה: תהי G חבורה מסדר סופי. הוכיחו שב- G יש איבר מסדר 2 אם $|G|$ זוגי.
 הוכחה: הסדר של איבר חייב לחלק את סדר החבורה. ולכן אם יש איבר מסדר 2, אז גודל החבורה הוא זוגי.

כעת, נניח ש- $|G|$ זוגי, ורוצים להוכיח שיש איבר מסדר 2.
 ניתן לחלק את החבורה לזוגות של איבר וההופכי שלו. אז e הוא ההופכי של עצמו. נשארנו עם כמות איזוגית, לכן חייב להיות לפחות איבר אחד שיופיע בזוג עם עצמו, וזה אומר שהוא מסדר 2.
 הגדרה: לכל $n \in \mathbb{N}$ נגדיר $\Omega_n = \{x \in \mathbb{C} : x^n = 1\}$ - שורשי היחידה מסדר n . זאת אכן תת חבורה עם פעולת כפל.
 למשל:

$$\Omega_2 = \{1, -1\}$$

$$\Omega_3 = \left\{1, \text{cis}\left(\frac{2\pi}{3}\right), \text{cis}\left(\frac{4\pi}{3}\right)\right\}$$

$$\Omega_4 = \{i, -i, 1, -1\}$$

נגדיר

$$\Omega_\infty = \bigcup_{n \in \mathbb{N}} \Omega_n$$

הוכיחו ש $\Omega_\infty \leq \mathbb{C} \setminus \{0\}$.
 הוכחה: Ω_∞ הוא בדיוק אוסף האיברים מסדר סופי ב $\mathbb{C} \setminus \{0\}$, והוכחנו שבחבורה אבלית אוסף האיברים מסדר סופי הוא תת חבורה.

הערה: זאת חבורה אינסופית, למעשה לכל מספר רציונלי $0 \leq \frac{n}{m} < 2$, יש בחבורה את $\text{cis}\left(\frac{n}{m}\pi\right)$.

ויש בה איבר מכל סדר סופי. כי לכל n , אפשר לקחת $\text{cis}\left(\frac{2\pi}{n}\right)$ משפט אוילר (מסקנה ממשפט לגרנז'): לכל n , $(x, n) = 1 \pmod n$, $x^{\varphi(n)} \equiv 1 \pmod n$.
 תרגיל: מצאו את 2 הספרות האחרונות של המספר

$$88211^{4039}$$

צריך למצוא

$$88211^{4039} \pmod{100}$$

ברור ש 2 ו 5 לא מחלקים את 88211, ולכן הוא זר ל 100.

$$\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$$

כלומר,

$$88211^{40} \equiv 1 \pmod{100}$$

$$88211^{4039} \pmod{100} = 88211^{4000} \pmod{100} \cdot 88211^{39} \pmod{100} =$$

$$(88211^{40})^{100} \pmod{100} \cdot 88211^{39} \pmod{100} =$$

$$(88211^{40} \pmod{100})^{100} \cdot 88211^{39} \pmod{100} =$$

$$(1 \pmod{100})^{100} \cdot 88211^{39} \pmod{100} =$$

$$= 88211^{39} \pmod{100}$$

נשים לב ש $88211^{39} \bmod 100 = 88211^{-1} \bmod 100$

$$88211 = 882 \cdot 100 + 11 \rightarrow 11 = 88211 - 882 \cdot 100$$

$$100 = 9 \cdot 11 + 1 \rightarrow 1 = 100 - 9 \cdot 11 = -9 \cdot 88211 + \dots$$

ולכן ההופכי הוא -9 . כלומר, במודולו 100 אפשר להעביר ל15.
לכן שתי הספרות האחרונות הן 91.